ABSTRACT

A combined digital signature is method of making a single public key digital signature on a number of messages, such that individual combined signatures may be extracted and individually presented. The mechanism of a combined digital signature is a combination of a hash tree whose leaves correspond to messages, together with a cryptographic signature made on the root of that hash tree. The invention comprises a method of making a combined signature, a method of extracting individual combined signatures, a method of verifying individual combined signatures, and the data format of an individual combined signature. The invention can increase performance of signature-making by a factor of several hundred over previous art.